

United States District Court
Central District of California

R.S.,

Plaintiff,

v.

PRIME HEALTHCARE SERVICES,
INC.,

Defendant.

Case № 5:24-cv-00330-ODW (SPx)

**ORDER GRANTING PLAINTIFF'S
MOTION FOR
RECONSIDERATION AND
DENYING DEFENDANT'S MOTION
TO DISMISS [26]**

I. INTRODUCTION

Plaintiff R.S. brought this putative class action against Defendant Prime Healthcare Services, Inc. ("Prime Healthcare") alleging violation of the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2511(1). (Compl., ECF No. 1.) The Court granted Prime Healthcare's Motion to Dismiss under Federal Rule of Civil Procedure ("Rule") 12(b)(6) and dismissed this action with prejudice. (Order Granting Mot. Dismiss ("Order"), ECF No. 24.) R.S. now moves for reconsideration of the Order under Rule 59(e) and Local Rule 7-18. (Mot. Recons. ("Mot." or "Motion"), ECF No. 26.) For the following reasons, the Court **GRANTS** R.S.'s Motion and, upon reconsideration, **DENIES** Prime Healthcare's Motion to Dismiss.¹

¹ Having carefully considered the papers filed in connection with the Motion, the Court deemed the matter appropriate for decision without oral argument. Fed. R. Civ. P. 78; C.D. Cal. L.R. 7-15.

II. BACKGROUND²

Prime Healthcare operates forty-four hospitals in fourteen states, including California, and more than 300 outpatient locations. (Compl. ¶ 1.) Prime Healthcare also owns, controls, and maintains websites and portals (collectively, “Web Properties”) that allow patients to communicate with their healthcare providers. (*Id.* ¶ 2.) These Web Properties allow patients to, among other things, access lab and test results, manage prescriptions, request refills, schedule and manage appointments, search for medical conditions and treatment options, and find doctors. (*Id.* ¶ 4.) R.S. alleges that, using tracking technologies, including Facebook pixels (“Pixels”), Prime Healthcare sent her—and other putative class members’—personally identifiable information and protected health information (“Private Information”) to Facebook and other third parties without patients’ knowledge or consent. (*E.g., id.* ¶¶ 8–14, 49–55, 122, 239.)

A. Facebook Pixels

Facebook encourages and promotes website owners, like Prime Healthcare, to use its “Business Tools” to market products and services to individuals. (*Id.* ¶ 97.) These Business Tools, including Pixels, are programming code advertisers can integrate into their webpages, mobile applications, and servers to collect user activity on those platforms. (*Id.* ¶ 98.) The Pixels send information from users’ browsers to third parties, including Facebook. (*Id.* ¶¶ 11, 99–100.)

Pixels are customizable: the website owner—here, Prime Healthcare—controls which of its web pages contain the Pixels and which events are tracked and sent to Facebook. (*Id.* ¶ 101.) Facebook configures the Pixels to collect “Standard Events,” such as when a user visits a particular webpage, the webpage’s URL and metadata, and button clicks. (*Id.* ¶ 106.) Website owners can also build “custom events” to track other user actions. (*Id.* ¶ 107.) The Pixels prompt users’ web browsers to send

²All factual references derive from Plaintiff’s Complaint, unless otherwise noted, and well-pleaded factual allegations are accepted as true for purposes of this Motion. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009).

1 users' communications with the host webpage to Facebook's servers. (*Id.* ¶ 108.)
2 This simultaneous transmission contains the electronic communications sent to the
3 host website and the data that the host configures the Pixels to collect. (*Id.* ¶ 109.)

4 When a Facebook user visits the website, the information the Pixels collect is
5 associated with that user's Facebook ID. (*Id.* ¶ 114.) The Facebook ID captures the
6 user's name and Facebook profile, which contains demographic and other information
7 about the user, including pictures, personal interests, work history, and relationship
8 status. (*Id.* ¶ 116.) The Pixels collect data even if the user does not have a Facebook
9 account: Facebook keeps "shadow profiles" on users without Facebook accounts. (*Id.*
10 ¶ 115.) After receiving these transmissions, Facebook processes, analyzes, and
11 assimilates the data into datasets. (*Id.* ¶ 114.)

12 Pixels allow website owners—like Prime Healthcare—to send targeted
13 advertisements to a user based on that user's Private Information. (*Id.* ¶ 19.) A
14 website owner can also target ads to users who have shown interest in its business and
15 measure the success of its marketing campaigns. (*Id.* ¶¶ 125–31.) The Pixels thus
16 enable "retargeting," or online marketing that targets users with ads based on prior
17 internet communications and interactions. (*Id.* ¶ 197.) Facebook also sells the
18 collected information, including Private Information, to third-party marketers who
19 target users' Facebook accounts based on that information. (*Id.* ¶ 20.)

20 **B. Prime Healthcare's Use of the Facebook Pixels**

21 R.S. alleges that Prime Healthcare installs Pixels on its Web Properties without
22 patients' knowledge. (*Id.* ¶ 8.) Using Pixels, Prime Healthcare intercepts patients'
23 Private Information and discloses this information to Facebook. (*Id.* ¶ 73.) For
24 example, when a patient searches for a doctor on Prime Healthcare's Web Properties,
25 the Facebook Pixels send the search information—here, the doctor's name—directly
26 to Facebook. (*Id.* ¶¶ 76–77.)

27 Prime Healthcare purchases Facebook's targeted advertising services to display
28 ads to Facebook users based on their health conditions. (*Id.* ¶¶ 117, 140.) At the same

1 time, Facebook sells these marketing profiles to third-party marketers to support
2 advertising efforts. (*Id.* ¶¶ 117, 195.) This financially benefits both Prime Healthcare
3 and Facebook. (*Id.* ¶ 118.) As R.S. alleges, “Prime Healthcare chose to use the Pixel
4 data for marketing purposes to bolster its revenue.” (*Id.* ¶ 24.)

5 **C. R.S.’s Claims**

6 R.S. has been a Prime Healthcare patient since approximately 2012. (*Id.* ¶ 231.)
7 R.S. began receiving healthcare services from Prime Healthcare and, starting in 2018,
8 accessed its Web Properties. (*Id.* ¶¶ 230–32.) She has had a Facebook account for at
9 least ten years. (*Id.* ¶ 234.) Through the Web Properties, R.S. scheduled
10 appointments, found doctors, researched medical treatments and conditions, and
11 provided personal health-related information. (*Id.* ¶¶ 230–33.) R.S. alleges that Prime
12 Healthcare disclosed her Private Information to Facebook without her knowledge,
13 consent, or written authorization, and in violation of the Health Insurance Portability
14 and Accountability Act (“HIPAA”). (*Id.* ¶¶ 8–9, 141–59.)

15 On February 8, 2024, R.S. filed this putative class action against Prime
16 Healthcare, asserting a single cause of action for violating the ECPA. (Compl.
17 ¶¶ 223–254, 256.) On April 24, 2024, Prime Healthcare filed a Motion to Dismiss
18 under Rule 12(b)(6), which Prime Healthcare opposed. (Mot. Dismiss, ECF No. 13;
19 Opp’n Mot. Dismiss, ECF No. 16; Reply ISO Mot. Dismiss, ECF No. 17.) On
20 August 7, 2024, the Court issued an Order granting Prime Healthcare’s Motion to
21 Dismiss and dismissed the case. (Order 1.) On August 8, 2024, the Court issued a
22 Judgment. (J., ECF No. 25.)

23 On August 21, 2024, R.S. moved for reconsideration of the Order pursuant to
24 Rule 59(e) and Local Rule 7-18. (Mot. 4–5.) The Motion is fully briefed. (Opp’n
25 Mot. (“Opp’n”), ECF No. 29; Reply ISO Mot. (“Reply”), ECF No. 30.)

26 **III. LEGAL STANDARD**

27 “Although Rule 59(e) permits a district court to reconsider and amend a
28 previous order, the rule offers an extraordinary remedy, to be used sparingly in the

1 interests of finality and conservation of judicial resources.” *Kona Enters., Inc. v. Est.*
2 *of Bishop*, 229 F.3d 877, 890 (9th Cir. 2000) (internal quotation marks omitted).
3 “Motions for reconsideration are governed by the Local Rules of this district.” *In re*
4 *Countrywide Fin. Corp. Mortg.-Backed Sec. Litig.*, 966 F. Supp. 2d 1031, 1036
5 (C.D. Cal. 2013). A party may move for reconsideration under Local Rule 7-18 if
6 there is: (a) “a material difference in fact or law from that presented to the [c]ourt that,
7 in the exercise of reasonable diligence, could not have been known to the party
8 moving for reconsideration at the time” the court entered the order, (b) “the
9 emergence of new material facts or a change of law occurring after” the court entered
10 the order, or (c) “a manifest showing of a failure to consider material facts presented
11 to the” court before it entered the order. C.D. Cal. Civ. L.R. 7-18; *In re Countrywide*,
12 966 F. Supp. 2d at 1036.

13 In seeking reconsideration, the movant may not “repeat any oral or written
14 argument made in support of, or in opposition to, the original motion.” C.D. Cal. Civ.
15 L.R. 7-18. “Consistent with Local Rule 7-18, a [Rule 59(e)] motion for
16 reconsideration should not be granted, absent highly unusual circumstances, unless the
17 district court is presented with newly discovered evidence, committed clear error, or if
18 there is an intervening change in the controlling law.” *Ketab Corp. v. Mesriani L.*
19 *Grp.*, No. 2:14-cv-07241-RSWL (MRWx), 2015 WL 2084469, at *2 (C.D. Cal.
20 May 5, 2015) (internal quotation marks omitted) (quoting *Carroll v. Nakatani*,
21 342 F.3d 934, 945 (9th Cir. 2003)); *Feltzs v. Cox Commc’ns Cal., LLC*, 562 F. Supp.
22 3d 535, 539 (C.D. Cal. 2021) (“Courts in this district have interpreted Local Rule 7-18
23 to be coextensive with Rules 59(e) and 60(b).”). “The Court has discretion in
24 determining whether to grant a motion for reconsideration.” *Feltzs*, 562 F. Supp
25 at 539.

IV. DISCUSSION

The Court first turns to R.S.'s argument that it should reconsider its ruling dismissing this action in the Order. Next, having found that reconsideration is proper, the Court addresses Prime Healthcare's Motion to Dismiss.

A. Reconsideration

R.S. moves for reconsideration of the Order under Rule 59(e) and Local Rule 7-18, arguing that the Court committed clear error by "fail[ing] to consider material facts presented to the Court before the Order was entered." (Mot. 6 (quoting C.D. Cal. L.R. 7-18).) Specifically, R.S. argues that the Court's failure to address the applicability of the crime-tort exception justifies reconsideration. (*Id.* at 6–8.) Prime Healthcare responds that the Court properly dismissed the Complaint and adequately addressed the crime-tort exception in its Order. (Opp'n 1.)

The ECPA provides for a private right of action against "any person who . . . intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a). "Intercept" is defined as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." *Id.* § 2510(4). The statute exempts from liability interceptions made by a person who "is a party to the communication" or when one of the parties to the communication consents to the interception. *Id.* § 2511(2)(d). This is often referred to as the "party exception" or "party exemption." *See, e.g., In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 607 (9th Cir. 2020). This exception is itself limited: it does not apply if the interception was "for the purpose of committing any criminal or tortious act," known as the crime-tort exception. *Sussman v. Am. Broad. Co., Inc.*, 186 F.3d 1200, 1202 (9th Cir. 1999) (quoting 18 U.S.C. § 2511(2)(d)).

In its Motion to Dismiss, Prime Healthcare argued that it is not liable under the ECPA because R.S. consented to Prime Healthcare intercepting her communications,

1 and thus the party exception applies. (Mot. Dismiss 1–2, 6–8.) R.S. countered that
2 the party exception does not apply because Prime Healthcare intercepted R.S.’s
3 communications with a criminal and tortious purpose, triggering the crime-tort
4 exception and precluding reliance on the party exception. (Opp’n Mot. Dismiss 6–9,
5 11–20.) Prime Healthcare disagreed, arguing that the crime-tort exception does not
6 apply here. (Mot. Dismiss 8–13; Reply ISO Mot. Dismiss 2–10.)

7 In its Order, the Court acknowledged that “R.S. argu[ed] extensively why the
8 ECPA’s crime-tort exception should in fact apply.” (Order 4.) But the Court did not
9 address these arguments. (*See id.*) Instead, the Court considered only the party
10 exception, concluding that Prime Healthcare was a party to the communication and
11 R.S. had consented to the interception. (*Id.* at 4–5.) But both parties agreed that if the
12 crime-tort exception applies, then the party exception cannot save Prime Healthcare
13 from R.S.’s claims. (*See* Mot. Dismiss 1; Opp’n Mot. Dismiss 7–8; *see also* Mot. 4;
14 Opp’n Mot. 7–9.) As the Court did not consider the applicability of the crime-tort
15 exception, the Court finds it appropriate to **GRANT** R.S.’s Motion under Local
16 Rule 7-18(c) and reconsider Prime Healthcare’s Motion to Dismiss. *See Kiwijet, LLC*
17 *v. Guangzhou Hayonex Int’l Logistics Co. Ltd*, No. 2:21-cv-07515-FWS (JDEx),
18 2024 WL 3468811, at *2 (C.D. Cal. May 22, 2024) (finding reconsideration
19 appropriate when the court determined that it failed to consider plaintiff’s opposition).

20 **B. Motion to Dismiss**

21 Having agreed to reconsider Prime Healthcare’s Motion to Dismiss, the Court
22 turns to Prime Healthcare’s argument that R.S. fails to plausibly allege that the
23 crime-tort exception applies, and thus that the party exception defeats R.S.’s claim.
24 (*See* Mot. Dismiss 9.)

25 As discussed, the crime-tort exception applies if a defendant intercepted a
26 communication “for the purpose of committing any criminal or tortious act.”
27 *Sussman*, 186 F.3d at 1202 (quoting 18 U.S.C. § 2511(2)(d)).
28

1 R.S. alleges that, at the time it intercepted her communications, Prime
2 Healthcare had the purpose to disclose private health information without her consent
3 in violation of HIPAA. (See Compl. ¶ 191 (alleging that Prime Healthcare embedded
4 the Pixels on its Web Properties “with the purpose of disclosing” users’
5 “communications to Facebook and other third party data brokers”); ¶¶ 141–59
6 (alleging Prime Healthcare intended to and did violate HIPAA).) According to R.S.,
7 “Prime Healthcare intentionally configured Pixels installed on its Web Properties to
8 capture both the characteristics of individual patients’ communications” and the
9 “content of these communications.” (*Id.* ¶¶ 71–73 (internal quotation marks
10 omitted).) Prime Healthcare argues that R.S. fails to allege sufficient facts to invoke
11 the crime-tort exception on three grounds: (1) there was no HIPAA violation,
12 (2) disclosure was not independent from interception, and (3) it held no improper
13 purpose. (See Mot. Dismiss 8–13.)

14 *1. HIPAA Violation*

15 Prime Healthcare first argues that R.S. does not plausibly allege that it violated
16 HIPAA. (Mot. Dismiss 10–12.) Prime Healthcare asserts that R.S. fails to allege that
17 it actually “disclosed” her confidential information to any third party. (*Id.* at 11.)
18 However, “the focus is not upon whether the interception itself violated another law; it
19 is upon whether the *purpose* for the interception—its intended use—was criminal or
20 tortious.” *Sussman*, 186 F.3d at 1202. So the question here is not whether Prime
21 Healthcare actually violated HIPAA, but whether it intended to do so.

22 R.S. plausibly alleges that Prime Healthcare intercepted her Private Information
23 with the purpose of violating HIPAA. HIPAA prohibits a “covered entity,” including
24 healthcare providers like Prime Healthcare, from knowingly “disclos[ing] individually
25 identifiable health information to another person.” 42 U.S.C. § 1320d-6(a)(3). R.S.
26 alleges that Prime Healthcare—through the Pixels—intended to collect her Private
27 Information, including her medical conditions, treatment details, appointment
28 information, and the physician she selected, and to disclose this Private Information to

1 third parties, including Facebook. (*Id.* ¶¶ 9, 11, 50, 69, 141–59, 240.) The Private
2 Information falls under HIPAA’s definition of “individually identifiable” information,
3 which includes data “created or received by a health care provider” that “[r]elates to
4 the past, present, or future physical or mental health or condition of an individual” or
5 to the “provision of health care to an individual.” 45 C.F.R. § 160.103.

6 Thus, Prime Healthcare’s argument that R.S. does not plausibly allege an intent
7 to “disclose” in violation of HIPAA fails. (*See* Compl. ¶¶ 141–59 (alleging
8 disclosure); *K.L. v. Legacy Health*, No. 3:23-cv-1886-SI, 2024 WL 4794657, at *6
9 (D. Or. Nov. 14, 2024) (finding intent to disclose private health information is a
10 “criminal act for purposes of the carve-out to ECPA’s party exception”); *Cooper v.*
11 *Mount Sinai Health Sys., Inc.*, No. 23 Civ. 9485 (PAE), 2024 WL 3586357, at *6
12 (S.D.N.Y. July 30, 2024) (holding that a plaintiff raising similar allegations
13 sufficiently alleged intent to disclose in violation of HIPAA).

14 2. Independence

15 Next, Prime Healthcare contends that the crime-tort exception is inapplicable
16 because “the interception did not precede the disclosure; it was the disclosure.”
17 (Reply ISO Mot. Dismiss 10.)

18 The crime-tort exception has two relevant components. First, there is a
19 “temporal” component whereby the intercepting party must “have the independent
20 criminal or tortious purpose *at the time* the [interception] was made.” *Planned*
21 *Parenthood Fed’n of Am., Inc. v. Newman*, 51 F.4th 1125, 1136 (9th Cir. 2022)
22 (emphasis added) (first citing *Sussman*, 186 F.3d at 1203; and then citing *Caro v.*
23 *Weintraub*, 618 F.3d 94, 99 (2d Cir. 2010)). This “temporal thread . . . runs through
24 the fabric of the statute and the case law.” *Caro*, 618 F.3d at 99. If “at the time of the
25 recording, the offender plans to use the recording to harm the other party to the
26 conversation, a civil cause of action exists” under the ECPA. *Id.* at 100.

27 Second, there is a “separate and independent” component whereby the crime or
28 tort intended must be “beyond the act of [intercepting] itself.” *Id.* at 98, 101 (“The

1 language and history of the Wiretap Act indicate that Congress authored the exception
2 to the one-party consent rule to prevent abuses stemming from *use* of the recording
3 not the mere *act* of recording.”). In other words, “the criminal or tortious acts
4 contemplated by § 2511(2)(d) are acts secondary to the acquisition of the
5 communication involving tortious or criminal use of the interception’s fruits.” *Pena v.*
6 *GameStop, Inc.*, 670 F. Supp. 3d 1112, 1120 (S.D. Cal. 2023) (quoting *In re Google*
7 *Cookie Placement Consumer Priv. Litig.*, 806 F.3d 125, 145 (3d Cir. 2015)). Thus, “at
8 the time of the” interception, a defendant must have “had an independent prohibited
9 purpose” beyond the act of interception itself for the crime-tort exception to apply.
10 *Weston v. Lefiti*, No. 23-cv-0896-L-DDL, 2023 WL 8458249, at *4 (S.D. Cal. Dec. 5,
11 2023) (citing *Sussman*, 186 F.3d at 1202), *aff’d*, No. 24-541, 2024 WL 4579237
12 (9th Cir. Oct. 25, 2024).

13 R.S. alleges facts to satisfy both requirements. First, R.S. alleges that, at the
14 time Prime Healthcare intercepted R.S.’s Private Information, it had the intent to
15 disclose that information in violation of HIPAA. (*See, e.g.*, Compl. ¶ 61 (alleging that
16 Prime Healthcare installed the Pixels and “programed or permitted those webpages to
17 surreptitiously share patients’ private and protected communications” with third
18 parties); ¶ 71 (alleging that “Prime Healthcare intentionally configured Pixels installed
19 on its Web Properties to capture” Private Information).) Second, R.S. alleges that
20 Prime Healthcare intended to violate HIPAA by disclosing Private Information to third
21 parties. (*See e.g., id.* ¶ 141 (alleging Prime Healthcare’s “disclosure” violated
22 HIPAA); ¶ 157 (describing unlawful “disclos[ure]”; *see also* Opp’n Mot. Dismiss 13.)

23 Prime Healthcare cites *Weston* to support its argument that the crime-tort
24 exception cannot apply here because its alleged HIPAA violation cannot be “based on
25 the interception.” (Reply ISO Mot. Dismiss 9 (citing *Weston*, 2023 WL 8458249,
26 at *4).) But that case supports R.S.’s position. In *Weston*, the plaintiff alleged that the
27 defendant’s recording of a phone call violated the plaintiff’s right to privacy and
28 caused emotional distress, extortion, and intentional interference with business

1 relationships. *Weston*, 2023 WL 8458249, at *4. The district court held that the
2 plaintiff failed to adequately allege “independent criminal or tortious purposes
3 separate from the act of recording” because the alleged harm, such as emotional
4 distress and invasion of privacy, directly arose from the act of recording itself. *Id.* In
5 other words, the plaintiff alleged his emotional distress resulted from defendant
6 making the recording itself, not from sharing the recording with others. *Id.* As the
7 Ninth Circuit explained in affirmance, emotional distress that “stem[s] from the mere
8 act of recording” does not support an allegation that an interception was done “for the
9 purpose of facilitating some further impropriety, such as blackmail.” *Weston*,
10 2024 WL 4579237, at *2.

11 Unlike the plaintiff in *Weston*, R.S. does not allege that Prime Healthcare’s
12 interception *itself* violated HIPAA. (See Compl.) Instead, R.S. asserts that the
13 violation stems from Prime Healthcare’s intentional *disclosure* of the collected Private
14 Information, which constitutes a “further impropriety” independent and separate from
15 Prime Healthcare’s *interception*. *Weston*, 2024 WL 4579237, at *2; (see Compl.
16 ¶ 157; Opp’n Mot. Dismiss 13.) This distinction places R.S.’s allegations squarely
17 within the crime-tort exception, as the intent to disclose private information predates
18 and is distinct from the interception itself. *Compare Caro*, 618 F.3d at 101 (holding
19 that invasion of privacy does not qualify for crime-tort exception because the “tort . . .
20 occurs through the act of interception itself” and “[n]othing more is required after the
21 interception is made for liability to attach based on this tort.”).

22 It is irrelevant that Prime Healthcare allegedly disclosed the Private Information
23 at the same time as its interception. (See Mot. Dismiss 9–10.) In so arguing, Prime
24 Healthcare conflates the crime-tort exception’s “separate and independent” component
25 with its “temporal” component. As discussed, the “temporal thread” focuses on when
26 the intent to disclose was formed. *See Caro*, 618 F.3d at 99 (“At the time of the
27 recording the offender must intend to use the recording to commit a criminal or
28 tortious act.”). Whether the disclosure occurs simultaneously with or shortly after the

1 interception, Prime Healthcare’s purpose remained the same at the time of the
2 interception: to disclose private information to third parties in violation of HIPAA. So
3 long as Prime Healthcare intended to disclose the information to a third party at the
4 time of interception, which R.S. plausibly alleges, Prime Healthcare’s argument fails.

5 3. *Purpose*

6 Finally, Prime Healthcare argues that it was motivated to use the Pixels to
7 increase profit and advance marketing, not to commit a crime or tort. (Mot.
8 Dismiss 12–13.) Prime Healthcare correctly raises that “[n]umerous courts have held
9 that increasing revenue and decreasing costs are not criminal or tortious endeavors.”
10 (*Id.* (collecting cases).)

11 Courts are divided as to whether a primary financial motivation shields an
12 intercepting party from liability under the ECPA. Some courts have found that the
13 “crime-tort exception is inapplicable where a defendant’s primary motivation is to
14 make money rather than to injure plaintiffs tortiously or criminally.” *Roe v. Amgen*
15 *Inc.*, No. 2:23-cv-07448-MCS (SSCx), 2024 WL 2873482, at *6 (C.D. Cal. June 5,
16 2024); *see, e.g., In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d 778, 797
17 (N.D. Cal. 2022) (“Multiple courts . . . have found that the crime-tort exception . . . is
18 inapplicable where the defendant’s primary motivation was to make money, not to
19 injure plaintiffs tortiously.”). Other courts have held that the “presence of a primary
20 financial motive” does not “inoculate[] a defendant from liability under the ECPA.”
21 *Cooper*, 2024 WL 3586357, at *9; *see, e.g., R.C. v. Walgreen Co.*, 733 F. Supp. 3d
22 876, 901 (C.D. Cal. 2024) (“[E]ven where a defendant is arguably motivated by
23 monetary gain, the crime-tort exception may nonetheless apply if plaintiffs have
24 adequately alleged that the defendant's conduct violated state law, including state law
25 privacy claims”).

26 The Court joins those courts that have held a monetary purpose does not
27 insulate a party from liability under the ECPA, at least at the motion to dismiss stage.
28 Here, R.S. alleges that Prime Healthcare was aware that disclosing intercepted Private

1 Information violates HIPAA but chose to do so for “marketing and analytics
2 purposes,” to generate profit. (Compl. ¶¶ 7, 19, 25, 69, 157.) Prime Healthcare’s
3 financial gain was contingent on disclosing HIPAA-protected information to third
4 parties. Legitimate objectives, like increasing revenue, do not shield a party from
5 liability for crimes or torts committed in the process. *See, e.g., Mekhail v. N. Mem’l*
6 *Health Care*, No. 23-CV-00440 (KMM/TNL), 2024 WL 1332260, at *5 n.4 (D. Minn.
7 Mar. 28, 2024) (“[T]he [c]ourt has serious doubts that a pecuniary purpose and an
8 injurious purpose can always be so clearly distinguished. And it defies common sense
9 that a clearly harmful act could escape liability as long as it was done for profit.”).

10 Take blackmail, which the Ninth Circuit gave as an example of an ECPA
11 violation. *See Sussman*, 186 F.3d at 1202 (“Where the [interception] is legal, but is
12 done for the purpose of facilitating some further impropriety, such as blackmail,” the
13 statute applies). Under Prime Healthcare’s reading, the ECPA would not prohibit a
14 person from intercepting a communication with the intent to use that communication
15 to blackmail so long as the ultimate reason for the blackmail was to make money.
16 There, the interceptor’s primary purpose would be to make money. And blackmail
17 would merely be a means by which to make money. Of course, this is often the end
18 goal for blackmail. *Cf. Blackmail*, BLACK’S LAW DICTIONARY (12th ed. 2024)
19 (providing historical definition as a “tax consisting of money, cattle, crops, or other
20 consideration” and providing as an example “threaten[ing] to expose a criminal act
21 unless I am paid money”). Under Prime Healthcare’s reading, blackmail would
22 rarely, if ever, violate the ECPA. This cannot be the case. *Cf. Sussman*, 186 F.3d
23 at 1202.

24 So too with HIPAA violations. While Prime Healthcare’s goal in violating
25 HIPAA may have been to make money, as alleged, its purpose of intercepting R.S.’s
26 Private Information, as alleged, was to disclose it to third parties. Prime Healthcare’s
27 financial motivation for disclosing R.S.’s Private Information does not immunize it
28 from liability under the ECPA. At this stage, by alleging these facts, R.S. has

1 plausibly raised that Prime Healthcare intercepted her Private Information with the
2 purpose of violating HIPAA, sufficient to satisfy the crime-tort exception.

3 **V. CONCLUSION**

4 For the reasons discussed above, the Court **GRANTS** R.S.'s Motion to
5 Reconsideration, (ECF No. 26), and **DENIES** Prime Healthcare's Motion to Dismiss
6 (ECF No. 13). Accordingly, the Court directs the Clerk to reopen the case. Prime
7 Healthcare shall file an answer to the Complaint within **twenty-one (21) days** of this
8 Order.

9
10 **IT IS SO ORDERED.**

11
12 January 13, 2025

13
14 
15 _____
16 **OTIS D. WRIGHT, II**
17 **UNITED STATES DISTRICT JUDGE**
18
19
20
21
22
23
24
25
26
27
28